

PERSONNEL & DOCUMENT SECURITY DIVISION

USDA/DA/OPPM/PDSD

Summer 2004

Seventh Edition



Special Interest Articles:

- Changes to the Security Briefing Notification process
- Information Security Training
- Completing the "Agency Use Block"



Individual Highlights:

SF 86C	2
SCI Access	3
GSA Containers	4
Interim Clearances	5
Visit Authorizations	6
Bulletin #04-02	8

Main Line (202) 720-7373

E-QIP Update

Electronic Questionnaires for Investigations

Processing (e-QIP) is finally here!

On Tuesday, June 29, 2004, the Office of Personnel Management (OPM) officially deployed e-QIP within USDA.

PDSD has joined efforts with the Agricultural Research Service, Office of Chief Information Officer, and the Office of Inspector General to kick off implementation of the electronic processing of security forms.

These offices are now fully equipped and ready to process Questionnaires for National Security Positions (Standard Form 86) via e-QIP. The processing of forms on a web-based application over a secure server will allow for faster processing of paperwork.

Once an employee completes the initial form in e-QIP, the data will be stored to repopulate the form whenever a follow-up investigation is due.

Security representatives from the Foreign Agricultural Service, Animal and Plant Health Inspection Service (APHIS), APHIS International, the Food and Nutrition Service, and the National Finance Center will attend e-QIP training in late August 2004.

For more information on becoming involved with the e-QIP program, please contact Susan Gulbranson at 720-7373.



Destruction of Classified National Security Information

Do you have classified national security information to destroy?

The National Security Agency (NSA) is responsible for testing and approving all destruction devices used to destroy classified national security information.

Recently, NSA began posting on their website the Evaluated Products List (EPL), which is a list of all devices tested and approved

for the destruction of classified national security information. You must use a device from this list.

The EPL can be found at:
<http://www.nsa.gov/ia/government/MDG/mdg00002.pdf>



Changes to the Security Briefing Notification Process



Since early 2003, the Personnel Security Branch (PSB) has been notifying the agency security Point-of-Contacts (POCs) via email when an employee's investigation has been favorably adjudicated and requires a National Security briefing before his/her security clearance can be granted. Upon receipt, the POCs would then forward the information to the employee for action.

In certain instances, PSB

Personnel Security Specialists have had to notify employees directly about completing a security briefing. These exceptions include emergency or rush requests, notification from the employees that they are not getting the information from their POCs, or due to an unclear POC designation.

In addition, we tend to receive individual handling requests from different POCs within the same agency. This causes confusion

among PSB staff members and a lack of uniformity when processing these time-sensitive notifications.

In order to streamline this process, PSB will now forward the briefing notifications directly to the employees with a cc: to the agency security POC. If the adjudicating specialist cannot locate an email address in MS Outlook, the email will be forwarded to the agency security POC for handling.

"We must not, in trying to think about how we can make a big difference, ignore the small daily difference we do make."

Marion Wright Edleman

Use of Standard Form 86 Certification (SF 86C)

The SF 86C Certification is a device for an individual to use to report changes to the most recent execution of the SF 86, Questionnaire for National Security Positions, when an update and review of SF 86 information are required.

OPM will not initiate investigations from the SF 86C form; however, information provided on this form may be reason to

require completion of a new SF 86 for the initiation of an investigation. **The SF 86C is *not* to be used as a substitution for the SF 86 when an individual is due for a reinvestigation.** OPM *must* have a newly prepared SF 86 to initiate the investigation requested by an agency official.

There are many situations where the SF 86C can be used when the sole purpose

is to determine if any information on a previously executed SF 86 has changed. For example, if an individual from another Federal agency has transferred into a position at your agency prior to the time their reinvestigation is due and you need an updated review of the SF 86 information to determine if there have been any changes that warrant an investigation.



"Need-to-Know" Definition

"Need-to-Know" refers to a determination made by a possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access

to, or knowledge, or possession of the classified information in order to perform tasks or services essential to the fulfillment of a U.S. Government program. Knowledge or possession of,

or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.



SCI Access Requirements

Sensitive Compartmented Information (SCI) is classified information concerning or derived from intelligence sources, methods, or analytical processes requiring handling exclusively within formal access control systems established by the Director of Central Intelligence (DCI).

Access to SCI is based on a clearly identified need-to-know, formal access approval, and an appropriate indoctrination. Once approved, the holder is expected to practice a need-to-know discipline in acquiring or disseminating SCI information.

To be considered for SCI access, an individual must be a U.S. citizen and his/her immediate family members must also be U.S. citizens. Exceptions to the U.S. citizenship requirements necessitate the completion of a *Letter of Compelling Need* to explain why the employee should receive the clearance despite the potential for foreign influence.

A Top Secret clearance, with a current SSBI investigation, is required prior to requesting SCI access.

A Standard Form (SF) 86, dated within the last two years, must accompany the request.

Individuals who hold SCI have special responsibilities and obligations to report to their security office any activities, conduct, or employment that could conflict with their ability to protect classified information from unauthorized disclosure.

When an approved employee no longer has a need-to-know due to reorganization, change in duties, or resignation, the SCI access approval must be canceled and the individual debriefed.

Contact Carrie Moore at 202/720-3487 with any questions.



Transferring Security Investigations

Federal agencies will normally accept another agency's investigation as the basis for granting a security clearance, provided your last security clearance investigation was completed within the past 5 years for a Top Secret clearance and 10 years for a Secret clearance, and you have not had a break in service of more than 2 years.

Also considered is whether there have been any significant changes in your situation since your last investigation. Some federal agencies might have additional investigative or

adjudicative requirements that must be met prior to their accepting a clearance granted by another agency.

If you have an employee transferring to USDA from another agency where they maintained an active investigation/clearance, note such information in the 'Remarks' field on the *Request for Personnel Security Services* form.

Provide as much information regarding the previous investigation as possible, to include the name of the investigating agency, the type of investigation that was

conducted, and the date the investigation closed.

In transfer situations, employees are still required to submit updated security questionnaires and releases.

If the previous investigation is current and adequate for the new position, PSB will request a copy of the investigation and review it upon receipt.

The updated questionnaire will be reviewed for any significant or derogatory changes.



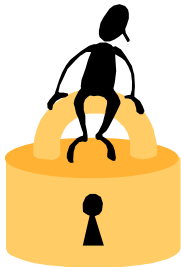
*“People are like tea bags.
You find out how strong
they are when you put
them in hot water.”*

Anonymous

GSA Approved Containers

ALL classified national security information must be stored in a GSA-approved security. Not sure if you have a GSA-approved security container? Contact the Information Security Staff and we will assist you in properly identifying your security container. We will also provide resources for purchasing new containers and assist you in making alternate storage arrangements until your new container arrives.

**DOES YOUR
CONTAINER LOOK
LIKE THIS?**



**DOES YOUR
COMBINATION DIAL
LOOK SIMILAR TO
THIS?**



**DOES YOUR
CONTAINER HAVE
LABELS LIKE THIS?**



*“To the man who only has
a hammer in his toolkit,
every problem looks like a
nail.”*

Abraham Maslow

DON'T FORGET!!!!

Combinations to security containers are classified at the same level as the highest level of information stored in that container. Combinations should be changed:

- When the container is made operational;
- When a person with access no longer requires that access, changes position, or retires;
- If you suspect the container has been tampered with or has been compromised; or
- On an annual basis – **WHICHEVER COMES FIRST**



Interim Security Clearance Requests

If deemed necessary and appropriate, the Personnel Security Branch may be able to grant an interim (temporary) security clearance to an employee while his/her investigation is processing at OPM.

Interim clearances are granted in exceptional circumstances where official functions must be performed before completion of the investigative and adjudicative processes associated with the security clearance procedure. There is no difference between an interim and a full security clearance as it relates to access to classified

information. However, when such access is granted, the background investigation must be expedited (35-day) service. If potentially disqualifying information is developed at anytime, the interim security clearance may be withdrawn.

An interim security clearance will be granted under the following conditions: 1) a demonstrated, clearly identified need stated on the *Justification for Requested Security Clearance* form; 2) a favorable review of the SF-86; 3) the submission of an appropriate 35-day investigation request to OPM; and 4) the completion

of a security indoctrination and signed SF312, Nondisclosure Agreement.

A request for interim SCI should be submitted only when there is an *emergency or urgent operational requirement* that necessitates indoctrination prior to the completion of the required investigation and the individual meets DCID 6/4 standards.

If you have any questions, please contact the Personnel Security Branch at 202/720-7373.



Periodic Reinvestigation Due Dates

Because circumstances and characteristics may change dramatically over time and thereby alter the eligibility of employees for continued access to classified information, reinvestigations shall be conducted with the same priority and care as initial investigations.

The reinvestigation due date is based on the closing date of the last investigation. This is not to be confused with the date the suitability determination or security clearance was granted.

For Top Secret and Critical-Sensitive/Secret clearances, reinvestigations are due every five years from the closing date of the prior investigation.

For Non-Critical Sensitive/Secret clearances, the reinvestigation is due every ten years from the closing date of the prior investigation.

For Confidential clearances, reinvestigations are due after a period of fifteen years from the closing date of the prior investigation.

Reinvestigation paperwork should be submitted to the Personnel Security Branch (PSB) about six months prior to the reinvestigation due date so that the request can be processed at OPM before the date lapses.

If you have any questions concerning reinvestigations, please contact Susan Gulbranson at 202/720-7373.

"The best executive is the one who has the sense to pick good men to do what he wants done, and self-restraint enough to keep from meddling with them while they do it."

Theodore Roosevelt



Information Security Briefings and Training

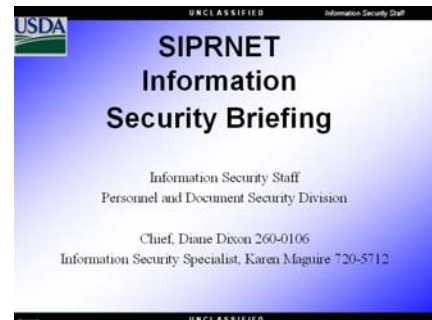
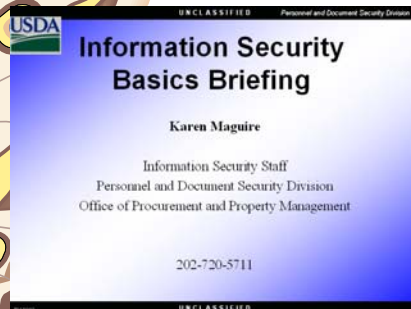
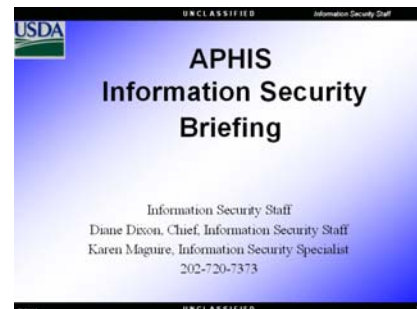
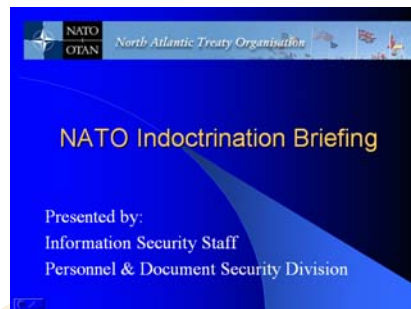
THE INFORMATION SECURITY STAFF (ISS) CREATES SPECIALIZED TRAINING FOR AGENCIES OR MISSION AREA.

CALL US TO SCHEDULE YOUR SPECIALIZED TRAINING NOW!!!

DIANE DIXON, CHIEF, ISS, 202-260-0106 OR KAREN MAGUIRE, ISS, 202-720-5712

"You can't build a reputation on what you are going to do."

Henry Ford



Classified Visit Authorizations

"In tempore pacis, para bellum – In time of peace, prepare for war."

Julius Caesar

Any visitors attending meetings or training in USDA facilities wherein classified information will be discussed *must* have their security clearance information forwarded to the Personnel Security Branch on official letterhead or via a visit authorization letter *prior* to the meeting.

Clearance information must be passed from the individual's security office (within an agency or company) to PDSD before the individual is cleared to attend the meeting.

The Personnel Security Branch (PSB) will confirm the authorization with the

USDA point-of-contact hosting the event that the visiting individuals have the necessary security clearance to attend the classified portions of the event.

Clearance verifications should be faxed to 202/720-7708 at least 48 hours prior to the meeting.



Instructions on completing the “Agency Use Block” on the SF86 and SF85P

Agency Use Information											
A Type of Investigation		B Extra Coverage		C Sensitivity Level		D Access		E Nature of Action Code		F Date of Action	Month Day Year
G Geographic Location		H Position Code		I Position Title							
J SON		K Location of Official Personnel Folder		None NPRC At SON		Other Address				Zip Code	
L SOI		M Location of Security Folder		None At SOI NPI		Other Address				Zip Code	
N OPAC-ALC Number				O Accounting Data and/or Agency Case Number							
P Requesting Official	Name and Title				Signature			Telephone Number ()		Date	

A (Type of Investigation): Enter the appropriate 3-character code for the type of investigation and service requested. The first two digits represent the investigation type, and the third digit represents the investigation service (A=35 days; B=75 days; C=120 days).

B (Extra Coverage): Enter the appropriate codes to represent the type of extra investigative coverage desired as follows:

**Code 7 (Attachments):* When information is attached to the investigative request such as miscellaneous documentation provided by the employee (INS, credit, diplomas).

**Code H (INS):* Automated scheduling of the Immigration and Naturalization Search. Place code “H” in Block B for this coverage. Use this code for all foreign-born employees.

**Code I (Spouse INS):* Automated scheduling of the Immigration and Naturalization Search for the subjects spouse. Place code “I” in Block B to request this coverage.

**Code R (Reinvestigation):* Place code “R” in Block B to indicate a reinvestigation.

C (Sensitivity Level): Enter one of the following codes representing the sensitivity level of the position requiring the investigation:

CODE LEVELS (SF86): 2 Non-Critical-Sensitive; 3 Critical-Sensitive; 4 Special-Sensitive

CODE LEVELS (SF85P): 5 Moderate Risk; 6 High Risk

D (Access Level): Enter the appropriate code from the chart below to show the type of security clearance/access the position requires.

CODE LEVELS (SF86): 0 Not Required; 1 Confidential; 2 Secret; 3 Top Secret; 4 Sensitive Compartmented Information

E (Nature of Action Code): If the person being investigated is a contract employee, enter “CON.”

I (Position Title): Enter the title of the position for which the investigation is being requested.

J (SON): Enter the 4 character Submitting Office Number (SON); For PDSD, this should be **AG00**.

K (Location of Official Personnel Folder): Check the correct box that gives us the location of the OPF.

NONE: If the person has never been a Federal employee, i.e. Contractors.

AT SON: **DO NOT** check this box. PDSD (AG00) is the Submitting Office. PDSD does not hold the employee OPF's.

OTHER ADDRESS: If the OPF is at any other location, furnish the address. All POC's must write in the address of the OPF location.

L (SOI): Enter the 4 character Security Office Identifier (SOI): **AG00**.

M (Location of Security Folder): Check the correct box that identifies the location of the Security folder.

NPI: If there is a security file at your agency, but it contains no pertinent information. This box should be checked for ALL requests.

N (OPAC-ALC Number) (On-Line Payment and Collection Agency Location Code): Enter your agency's OPAC-ALC number that records the billing information.

O (Accounting Data): You may enter your agency data for internal use (internal case number, file number, MO#, etc.).

P (Requesting Official): Leave these fields blank. OPM will contact this person concerning specific case related submission problems. PDSD will complete this block.



Personnel & Document Security Division

1400 Independence Ave, SW
RM S-310
Washington, DC 20250

Phone:
(202) 720-7373

Fax:
(202) 720-7708

E-mail:
pdsd@usda.gov

We're on the Web!

See us at:

<http://www.usda.gov/da/pdsd/>

Proper Position Designation Importance

Proper position risk and sensitivity designations are the foundation of effective and consistent suitability and security programs. Position designations determine the type and level of investigation required for proper screening of an individual for each USDA position.

All positions must have a risk designation based on the duties and responsibilities of the position.

Position designations ensure that proper investigations are performed in compliance with 5 CFR 731, 732, 736, Executive Order 10450, and Executive Order 12968.

Questions regarding the risk or sensitivity designation for an employee's position should be directed to your Human Resources office, which should maintain a *Position Designation Record* for every position in their department.

New PSD Bulletin #04-02: National Security Clearances for USDA Contractor Employees

Effective July 10, 2004, the USDA will no longer grant national security clearances to federal contractor personnel (non-USDA employees). The sole exception concerns individual consultants on contract to USDA (where the contract is between USDA and that individual, as opposed to a contract with a company employing that individual). All national security clearance investigations currently in process with the OPM will be continued through to completion and PSDS will grant final security clearances. PSDS will return to submitting agencies any contractor investigative requests that are received hereafter. To view this bulletin, visit the PSDS web site at <http://www.usda.gov/da/pdsd/bulletins.htm>.

Fingerprint Submission

Fingerprint charts are occasionally returned 'unclassifiable' (not readable) by the FBI.

When this occurs, OPM sends a "**Notification of Unclassifiable Prints**" form to PSB requiring a second submission of a fingerprint

chart to meet OPM standards.

Agencies are encouraged to submit two fingerprint charts with their original *Request for Personnel Security Services* package in order to minimize any processing delays.

In addition, please ensure that you are submitting the correct fingerprint chart in relation to the job status as follows:

SF 87 (federal employees)

FD 258 (contractors)

TO AVOID THE REJECTION OF FINGERPRINTS BY THE FBI AS "UNCLASSIFIABLE," EXAMINE THE FINGERPRINT IMPRESSIONS AFTER THEY ARE TAKEN, LOOK FOR THESE CHARACTERISTICS OF GOOD PRINTS:

- 1) Are the fingerprint ridges clearly visible on each print or are the fingerprint impressions too dark or too light?
- 2) Are the fingerprints clear and "in focus" or do they appear smudged?
- 3) Were the fingers fully rolled from the nail on one side to the nail on the other side? If the fingers were properly rolled, each individual print will have a square appearance in the boxes.
- 4) If some physical or skin condition makes it impossible to get perfect impressions, the person taking the fingerprints should indicate "Best Prints Possible" due to _____, on the card.

